RANDORISEC

Advanced Penetration Testing in Real World

Description :

Guillaume and Davy, senior pentesters, will share many techniques, tips and tricks to deliver to pentesters, red teamers bug bounty researchers or even defenders during a 2 days 100% “hands-on” workshop.
This is the exact training that you would have liked to have before wasting your precious time trying and failing while testing.

Main topics of the training are:

- **buffer overflow 101**: find and exploit buffer overflows yourself and bypass OS protections (because a lot of pentesters don’t even know how it works under the hood);
- **web exploitation**: manually find and exploit web app vulnerabilities using Burpsuite (yes, running WebInspect, AppScan, Acunetix or Netsparker is fine but you can do a lot more by hand);
- **network exploitation**: manually exploit network related vulnerabilities using Scapy, *ettercap and Responder (because it works so often when doing internal pentests);
- **passwords**: optimize the way you attack offline and online passwords (0day is fun but the way guys come in most of the time is simply by using login/passwords);
- **mobile app hacking**: find and exploit Android/iOS app vulnerabilities using Needle, Frida, Cycript and Hopper (companies move their apps in the cloud and in the mobile world so pentesters have to evolve with that… or die);

Duration :

2 days (approx. 14h)

Public :

Auditors / pentesters